

# Practical quantum random number generator based on sampling vacuum fluctuations

Qiang Zhou,<sup>1,2</sup> Raju Valivarthi,<sup>1,2</sup> Caleb John,<sup>1,3</sup> and Wolfgang Tittel<sup>1,2</sup>

<sup>1</sup>*Institute for Quantum Science and Technology, and Department of Physics & Astronomy,  
University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada*

<sup>2</sup>*Department of Physics and Astronomy, University of Calgary, Calgary, AB, T2N 1N4, Canada*

<sup>3</sup>*Department of Electrical and Computer Engineering,  
University of Calgary, Calgary, AB, T2N 1N4, Canada*

(Dated: March 3, 2017)

Quantum random number generation is an enabling technology for applications of quantum information science. For instance, a secure quantum key distribution (QKD) system requires a practical, easily integratable, high-quality and fast random number generator. Here, we propose and demonstrate an approach to random number generation that promises to satisfy these requirements. In our scheme, vacuum fluctuations of the electromagnetic-field inside a laser cavity are sampled in a discrete manner in time and amplified by injecting current pulses into the laser. This results in the generation of laser pulses with random phases. Random numbers can be obtained by interfering the laser pulses with another independent laser operating at the same frequency. Using only off-the-shelf opto-electronic and fiber-optic components at 1.5  $\mu\text{m}$  wavelength, we demonstrate experimentally the generation of high-quality random bits at a rate of up to 1.5 GHz. With the help of better opto-electronic devices, the generation rate of our scheme can be improved up to tens of GHz. Our results show the potential of the new scheme for practical quantum information applications.

## I. INTRODUCTION

The generation of true random numbers is highly desirable for digital information systems [1–3]. For instance, in quantum key distribution (QKD), random bits are used as a seed for creating secure keys shared between two legitimate users [4–6]. Devices generating random numbers by exploiting the unpredictable nature of quantum processes are known as quantum random number generators (QRNGs) [7–9]. Among all quantum physical systems, photons are possibly the most promising medium as they are easy to generate, manipulate and detect. Taking advantage of current photonics technology, QRNGs have been demonstrated based on the detection of single photon in different modes [10–18], quantum non-locality of entangled pairs of photons [19, 20], phase noise of lasers [21–24], vacuum-seeded bistable processes [27, 28], vacuum states [25, 26], and vacuum fluctuations in laser cavities [29–33]. Yet, despite intense efforts to develop high-quality and high-speed QRNGs, more work is required for creating simple, cost-effective and practical devices.

In this Letter, we propose and experimentally demonstrate a quantum random number generation scheme

that is based on the creation of short laser pulses with quantum-random phases [34]. QRNGs based on such phase randomness have been demonstrated before: by interfering subsequent pulses in an unbalanced Mach-Zender interferometer (UMZI), the phase randomness was mapped onto easily-detectable intensity variations [30–33]. However, due to pulse emission-time jitter, the interference quality degrades significantly as the pulse length approaches the emission-time uncertainty, which limits the minimum pulse width and hence the maximum pulse rate [31, 33]. In our scheme, the phase randomness of laser pulses is converted into intensity fluctuations by interfering them with another (quasi)-continuous wave laser featuring identical central frequency and polarization. The restriction of data acquisition to short time windows aligned – possibly after pulse detection – with the centres of the laser pulses effectively broadens and equalizes the spectra of the continuous wave laser and the pulsed laser, thereby ensuring high interference contrast even at high pulse repetition rates. Thus, our method not only inherently guarantees the temporal overlap needed for good interference, but can also create random numbers with narrower laser pulses and hence higher generation rates. Using only off-the-shelf opto-electronic and fiber-optic components at 1.5  $\mu\text{m}$  wavelength, we perform a proof-of-principle experiment of the proposed scheme and extract high-quality quantum random numbers at a rate of 1.5 GHz. Moreover, we discuss ways to improve the performance, i.e. the generation rate, of our scheme.

## II. PROPOSED SCHEME

Figure 1 (a) shows the idealized schematic of our random number generation. A semiconductor laser,  $L1$ , is operated in gain-switched mode. It is first biased far below threshold, i.e. around 0 mA, and then driven significantly above threshold using a short current pulse. This pulse samples and amplifies the vacuum fluctuation of the electromagnetic-field in the laser cavity, which results in the generation of laser pulses with quantum-random phases. Pulses from  $L1$  are then superposed with the output of a (quasi)-continuous wave laser,  $L2$ , using a 50/50 beam splitter (BS). Note that an optical isolator (ISO) is used to avoid all light injecting into  $L1$ , thereby preventing the generation of phase correlations between laser pulses [37, 38].

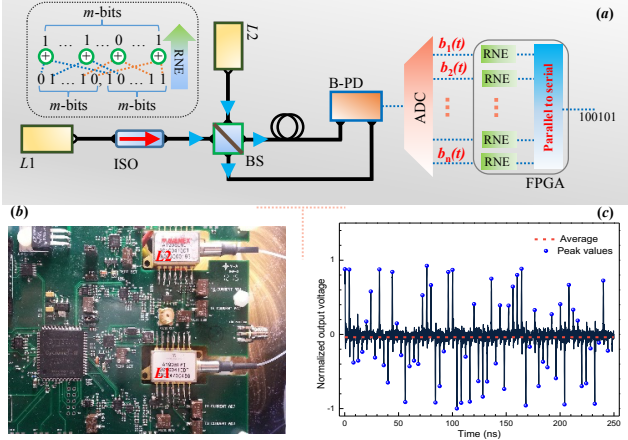


FIG. 1. (a) Schematic of our random number generator; (b) Picture of PCB board with gain-switched (pulsed) laser and (quasi)-continuous wave laser; (c) Typical signal from balanced-photo detector.  $L1$ : gain-switched laser;  $L2$ : (quasi)-continuous wave laser; ISO: optical isolator; BS: 50/50 beam splitter; B-PD: balanced-photo detector; ADC: analog to digital converter; RNE: randomness extractor; XOR: exclusive OR gate; VEDL: variable electronic delay line; SW: switch; CLK: clock; FPGA: field programmable gate array.

The interfering pulses are detected by a balanced photo detector (B-PD). Ignoring detector noise, the differential voltage  $\Delta V(t)$  output by the B-PD is

$$\Delta V(t) = 4 \times \eta_d E_1(t) E_2(t) \sin[\varphi_1(t) - \varphi_2(t)], \quad (1)$$

where  $\eta_d$  is the efficiency of the B-PD;  $E_1(t)$ ,  $E_2(t)$ ,  $\varphi_1(t)$  and  $\varphi_2(t)$  are the amplitudes and phases of the light fields from  $L1$  and  $L2$ , respectively; and  $t = MT$ , where  $M$  is an integer and  $T$  is the pulse period of  $L1$ . Since  $\varphi_1(t)$  is random, electrical pulses of random amplitudes are obtained from B-PD.

To convert the pulses into raw bits, each pulse is input into an analog-to-digital converter (ADC) that divides the range of possible amplitudes into  $2^n$  bins. (As we explain later, the maximum effective number of bins,  $2^{n_{max}}$ , that can be achieved is determined by the min-entropy of the signal from the B-PD [30].) The output of the ADC, specified by  $n$  bits  $b_1, b_2, \dots, b_n$ , is then sent into a field programmable gate array (FPGA) that performs a randomness extraction procedure, resulting in true quantum-random bits. This procedure requires  $n$  randomness extractors (RNEs). Each RNE receives one specific bit  $b_i(t)$  per ADC output (see Fig. 1 (a)). The RNE buffers  $2m$  bits during  $2m$  periods, then divides them into two  $m$ -bit strings, for example  $b_i(T), \dots, b_i(mT)$  and  $b_i(mT + T), \dots, b_i(2mT)$ . The two  $m$ -bit strings are then input into an XOR gate, where elements are XORed element wise, for e.g.  $b_i(T)$  with  $b_i(mT + T)$ ,  $b_i(2T)$  with  $b_i(mT + 2T)$  and so on. This creates  $m$  bits at the output, as shown in the inset of Fig. 1 (a). The value of  $m$

determines the separation between the two bits that are combined in the XOR gate. A larger  $m$  means less correlation between bits. Hence, with a proper value of  $m$ , the method presented here is equivalent to using two independent raw-bit sources, as demonstrated in Ref. [27]. Finally, after parallel-to-serial conversion, the bits from all RNEs form a string of ready-to-use random bits. Thus we can achieve an average generation rate of random numbers of  $nR/2$ , where  $R = 1/T$  is the repetition rate of the pulsed laser  $L1$ . We note that, compared with randomness extraction using a cryptographic hash function [39], the employed RNE method in our scheme imposes less performance on the FPGA and is much easier to implement in real time. However, it may result in losing more random bits than necessary to obtain a final quantum-random bit string.

### III. PROOF-OF-PRINCIPLE DEMONSTRATION

Figure 1 (b) shows a picture of the laser drivers and lasers  $L1$  and  $L2$  used in our experimental demonstration of the proposed scheme. The central wavelengths of both lasers are at 1540 nm – they are matched and stabilized by controlling the lasers' temperatures within 0.01 °C. The gain-switched laser is driven by a sequence of current pulses, which are generated from a radio-frequency transistor switched on/off by an FPGA signal. The width of the current pulse is  $\sim 200$  ps, and the repetition rate is 250 MHz. After interference with the output from the (quasi)-continuous wave laser  $L2$  in a polarization maintaining 50/50 BS (used to match the polarization mode, thus maximize the visibility), the optical signals are detected by a commercial B-PD (Thorlabs, PDB480C). It is worth noting that the balanced detection scheme removes all common-mode noise, which results in the improvement of the signal-to-noise ratio of the detection signal. Figure 1 (c) shows typical signals from B-PD, i.e.  $\Delta V(t)$  given in Eq. (1). The dashed line is the average of the detected signal.

Please note that, in our proof-of-principle demonstration, the ADC, RNEs and parallel-to-serial conversion described above have not been implemented using an FPGA. Instead, we used a computer to process analog signals from B-PD that have previously been sampled by a fast oscilloscope (Lecroy, 8600A). Hence, while we demonstrate a proof-of-principle of the proposed scheme, the random numbers are not yet generated in real time.

### IV. RESULTS

As shown in Eq. (1), the phase uncertainty of the emitted laser pulses affects  $\Delta V(t)$  through the interference and balanced photo-detection. Figure 2 shows the probability density function (PDF) of the normalized  $\Delta V(t)$ , sampled at pulse center  $t = mT$ . The dots

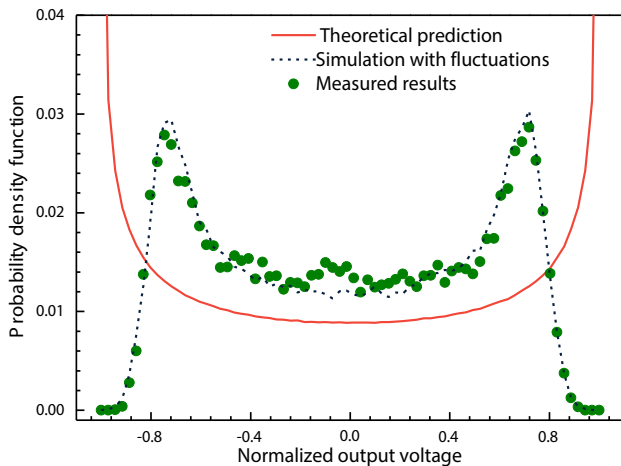


FIG. 2. Probability density function of the normalized analog signals,  $\Delta V(t)$

represent the experimental results. The solid red line is the theoretical prediction of the corresponding PDF, i.e.  $p(x) = 1/(\pi\sqrt{1-x^2})$ , where  $x$  is the normalized analog output of the B-PD at  $t=mT$ , and the phase distribution is assumed to be uniform. We attribute the deviation of our experimental results from the theoretical prediction to additional amplitude fluctuations in the detection signal that stem from classical sources, such as peak power fluctuations of laser pulses, limited bandwidth of the B-PD, finite sampling rate, and noise of the oscilloscope. We estimate the extent of these amplitude fluctuations by inputting the laser pulses from  $L1$  into one of the photo-detectors of the B-PD and analyzing its output using the same oscilloscope. Ideally, without the above-mentioned fluctuations, we would expect a constant output from that detector. However, we found an electrical signal whose amplitude follows a Gaussian distribution with standard deviation of  $\leq 5\%$  compared to the full range of the observed electrical signal. We simulate the effect of these classical fluctuations by adding them to the predicted values for the ideal case using a Monte-Carlo method. The dashed line in Fig. 2 shows the good agreement of the result with the measured data. This allows us not only to verify that the phase of each pulse is indeed random (but not fully quantum-random), but also suggests ways to improve the quality of the random numbers, such as using a B-PD and ADC with large bandwidth.

One of the main advantages of this random number generation scheme is that more than one random bit can be obtained per detection. The total range of the measured signal can be divided into  $2^n$  bins, and each signal represented by  $n$  bits. The maximum number of bits,  $n_{max}$ , that can be extracted is determined by the min-entropy of the analog signal from B-PD,

$$H_{min} = -\log_2(p_{max}) \quad (2)$$

where  $p_{max}$  is the maximum probability for the detec-

tion amplitude to belong into any of the  $2^n$  bins. By increasing the number of bins, we find that  $H_{min}$  saturates at 12.8 for  $n \geq 13$ , indicating that  $n_{max} = 12$  raw random bits can be extracted from each pulse [30]. However, please recall that these 12 bits originate from combined quantum and classical noise, with the classical noise of 5% corresponding to about  $12 \times H_2(0.05)$  bits = 3.43 bits, where  $H_2(x)$  denotes the binary entropy function. To remove the classical contribution, we employ the randomness extraction procedure described in section II, which reduces the information per laser pulse from 12 to 6 bits – significantly exceeding the requirement of 3.43 bits. Therefore, with a clock rate of 250 MHz, 12-bit binning and the randomness extraction, random bits are obtained at 1.5 GHz rate, which is half of the maximum of 3.0 GHz =  $12 \times 250$  MHz.

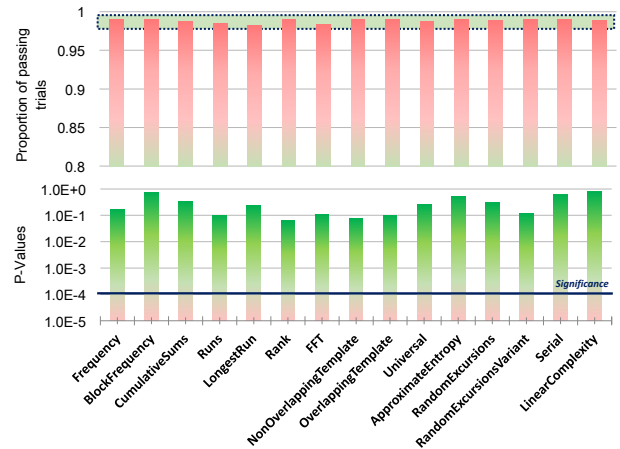


FIG. 3. Results of the NIST tests applied to 1.25 Gbits of random bits. (a) The proportion of passes of each test for 1000 1-Mb-long samples. All tests are passed with a proportion value greater than 0.9806 and less than 0.9994; (b) the P-values of each individual test, obtained from the distribution of P-values of each of the 1000 trials. All tests are passed with 1000 1-Mb-long samples and at a significance level of 0.0001. For the tests, which produce multiple P-values and proportions, the worst cases are given.

To show the quality of the final random bits obtained from our setup, we first create a 1 Gbit-long random file by saving measurement results from the oscilloscope and processing them in the computer. This random file is then subjected to the NIST statistical suite, which is a battery of fifteen tests used to analyze the statistical properties of random numbers [40]. By monitoring the results of the NIST test as a function of  $m$  (i.e. the length of the buffer in the RNEs), we find that with  $m = 7$ , the obtained random file passes all the tests.

For the NIST test, the significance level ( $\alpha$ ) is set at 0.01 as suggested by the test suite [40], implying that one out of one hundred tests is expected to fail even if the random numbers being tested are generated by a fair

random generator. Each of the fifteen tests is considered to be a success if the proportion of success versus fail is within a range given by  $\hat{p} \pm 3\sqrt{\hat{p}(1-\hat{p})/N}$ , where  $N$  is the number of times an individual test runs (i.e.  $N = 1000$  in our case), and  $\hat{p} = 1 - \alpha$ . This results in the proportion value greater than 0.9806 and less than 0.9994 in our case, which is the range of green-dashed bar as shown in Fig. 3 (a). Next, a P-value is obtained for each test from the distribution of P-values over 1000 trials. It is considered a pass if this P-value is above the suggested significance level of 0.0001 [32]. As shown in Fig. 3, our data passes all the NIST tests.

## V. CONCLUSION

We introduced and reported a proof-of-principle demonstration of a new scheme for creating high quality quantum-random bits based on a gain-switched and a (quasi)-continuous wave laser. The generation rate, currently 1.5 Gbps, can be further increased by operating the gain-switched laser with higher repetition rate. While this rate is fundamentally limited due to the need for laser cavity depletion in-between subsequent pulses, rates of several GHz for gain-switched laser are feasible

[32, 33]. Combined with the possibility to create more than 10 random bits per laser pulse, we therefore predict that our scheme can deliver high-quality quantum random numbers at rates of many tens of GHz.

We note that, while the present work was being finalized, a related experimental demonstration using a photonics chip has been reported [41, 42].

## FUNDING INFORMATION

This work was funded through Alberta Innovates Technology Futures (AITF), and the National Science and Engineering Research Council of Canada (NSERC). WT furthermore acknowledges funding as a Senior Fellow of the Canadian Institute for Advanced Research (CIFAR).

## ACKNOWLEDGMENTS

The authors thank Vladimir Kiselyov for technical support, and Daniel Oblak and Carlos Abellán for useful discussions.

- 
- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **175**, 8(1984).
  - [2] N. Metropolis and S. Ulam, "The Monte Carlo Method," Journal of the American Statistical Association **44**, 335(1949).
  - [3] B. Schneier and P. Sutherland, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, (John Wiley & Sons, 1995).
  - [4] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145(2002).
  - [5] N. Gisin and R. Thew, "Quantum communication," Nature Photonics **1**, 165(2007).
  - [6] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nature Photonics **8**, 595(2014).
  - [7] H. Schmidt, "Quantum mechanical random number generator," Journal of Applied Physics **41**, 462(1970).
  - [8] H.-C. Miguel and G.-E. Juan, "Quantum random number generators," arXiv:1604.03304v1, quant-ph(2016).
  - [9] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Information **2**, 16021(2016).
  - [10] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter and A. Zeilinger, "A Fast and Compact Quantum Random Number Generator," Rev. Sci. Instrum. **71**, 1675(2000).
  - [11] M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan, D. A. Ritchie and A. J. Shields, "Efficient and robust quantum random number generation by photon number detection," Appl. Phys. Lett. **107**, 071106(2015).
  - [12] J. F. Dynes, Z. L. Yuan, A. W. Sharpe and A. J. Shields, "A high speed, post processing free, quantum random number generator," Appl. Phys. Lett. **93**, 031109(2008).
  - [13] M. A. Wayne and P. G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," Optics Express **18**, 9351(2010).
  - [14] H. Furst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer and H. Weinfurter, "High speed optical quantum random number generation," Optics Express **18**, 13029(2010).
  - [15] M. Wahl, M. Leifgen, M. Berlin, T. Rhlicke, H.-J. Rahn and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," Appl. Phys. Lett. **98**, 171105(2011).
  - [16] B. Sanguinetti, A. Martin, H. Zbinden and N. Gisin, "Quantum Random Number Generation on a Mobile Phone," Phys. Review X **4**, 031056(2014).
  - [17] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann and H. Zbinden, "Quantum Random Number Generation for 1.25-GHz Quantum Key Distribution Systems," Journal of Lightwave Technology **33**, 2855(2015).
  - [18] Z. Cao, H. Zhou, X. Yuan and X. Ma, "Source-Independent Quantum Random Number," Phys. Rev. X **6**, 011020(2016).
  - [19] S. Pironio, A. Acin, S. Massar, A. B. Giday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021(2010).
  - [20] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden and N. Brunner, "Self-

- Testing Quantum Random Number Generator,” *Phys. Rev. Lett.* **114**, 150501(2015).
- [21] B. Qi, Y.-M. Chi, H.-K. Lo and L. Qian, “High-speed quantum random number generation by measuring phase noise of a single-mode laser,” *Optics Lett.* **35**, 312(2010).
  - [22] H. Guo, W. Tang, Y. Liu and W. Wei, “Truly random number generation based on measurement of phase noise of a laser,” *Phys. Rev. E* **81**, 051137(2010).
  - [23] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang and J.-W. Pan, “The generation of 68 Gbps quantum random number by measuring laser phase fluctuations,” *Rev. Sci. Instrum.* **86**, 063105(2015).
  - [24] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng and H.-K. Lo, “Ultrafast quantum random number generation based on quantum phase fluctuations,” *Optics Express* **20**, 12366(2012).
  - [25] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Maurer, U. L. Andersen, C. Marquardt and G. Leuchs, “A generator for unique quantum random numbers based on vacuum states,” *Nature Photonics* **4**, 711(2010).
  - [26] Y. Shi, B. Chng and C. Kurtsiefer, “Random numbers from vacuum fluctuations,” *Appl. Phys. Lett.* **109**, 041101(2016).
  - [27] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura and P. Davis, “Fast physical random bit generation with chaotic semiconductor lasers,” *Nature Photonics* **2**, 728(2008).
  - [28] A. Marandi, N. C. Leindecker, K. L. Vodopyanov and R. L. Byer, “All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators,” *Optics Express* **20**, 19322(2012).
  - [29] T. Symul, S. M. Assad and P. K. Lam, “Real time demonstration of high bitrate quantum random number generation with coherent laser light,” *Appl. Phys. Lett.* **98**, 231103(2011).
  - [30] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell and V. Pruneri, “True random numbers from amplified quantum vacuum,” *Optics Express* **19**, 20665(2011).
  - [31] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M.-W. Mitchell, “Generation of fresh and pure random numbers for loophole-free Bell tests,” *Phys. Rev. Lett.* **115**, 250403(2015).
  - [32] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri and M. W. Mitchell, “Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode,” *Optics Express* **22**, 1645(2014).
  - [33] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews and A. J. Shields, “Robust random number generation using steady-state emission of gain-switched laser diodes,” *Appl. Phys. Lett.* **104**, 261112(2014).
  - [34] K. Y. Lau, “Gain switching of semiconductor injection lasers,” *Appl. Phys. Lett.* **52**, 257(1988).
  - [35] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, “Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks,” *Phys. Rev. Lett.* **111**, 130501(2013).
  - [36] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, “Experimental Measurement-Device-Independent Quantum Key Distribution,” *Phys. Rev. Lett.* **111**, 130502(2013).
  - [37] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo and L.-M. Liang, “Effect of source tampering in the security of quantum cryptography,” *Phys. Rev. A* **92**, 022304(2015).
  - [38] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Pentty, and A. J. Shields, “Quantum key distribution without detector vulnerabilities using optically seeded lasers,” *Nature Photonics*, doi:10.1038/nphoton.2016.50 (2016).
  - [39] N. Nisan and A. Ta-Shma, “Extracting randomness: a survey and new constructions,” *J. Comput. Syst. Sci.* **58**, 148-173 (1999).
  - [40] A. Rukhin, et al. “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” (Special Publication 800–22 Revision 1, National Institute of Standards and Technology, 2008).
  - [41] C. Abellán, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. Mitchell, and V. Pruneri, “A quantum entropy source on an InP photonic integrated circuit for random number generation,” arXiv:1609.03255v1, quant-ph(2016).
  - [42] Our scheme employs laser pulses of a few tens of picoseconds length, created at 250 MHz without applying a current bias to the laser diode. In contrast, C. Abellán et al. use five nanosecond-long laser pulses created by superimposing a 10 mA bias current with a 100 MHz current modulation. In addition to different pulse generation rates, it is conceivable that the phase correlations between subsequent pulses are not be the same in the two schemes. We furthermore note that C. Abellán et al. assessed the entropy of their source, but did not actually generate random bits and test their quality.